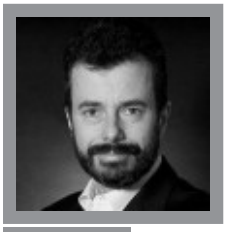
The Wayback Machine - https://web.archive.org/web/20210420231001/https://www.ingenium-magazine.it/s...

TECH VISION | 28 MAG 2019

Smart contract: cosa sono e a cosa servono

La Blockchain crea applicativi che possono facilitarci la vita. Ma con qualche criticità ancora da risolvere



CARLO PIANA
@carlopiana

GIORGIO ALESSANDRO DONÀ DANIONI

Accept

Quando si parla di Blockchain, il pensiero della maggior parte degli utenti si rivolge subito alle criptovalute e quindi al Bitcoin. Tuttavia la tecnologia che ha dato origine al Bitcoin ha ben più vaste applicazioni delle criptomonete. Tra quelle con un elevato potenziale ci sono gli Smart contract.

Registro distribuito, pubblico, aperto

Come noto, la Blockchain realizza un registro di dati (con qualsiasi dato e di qualsiasi tipo) aggiornato da tutte le persone che vogliano utilizzarlo, senza necessità di un'autorità centrale che ne controlli l'aggiornamento. Un registro distribuito, ovvero presente in molte copie tutte ugualmente "vere", purché rispettino i protocolli e conservino l'integrità garantita dalla continuità dei blocchi legati l'uno all'altro dalla serie di impronte digitali o "hash". Un registro di dati, dunque, pubblico e trasparente, fatto in modo che qualsiasi persona vi possa accedere per controllare tutti i dati scritti all'interno. Un registro non alterabile, perché per la natura stessa del registro vi sarebbe bisogno di uno sforzo tecnico che renderebbe l'operazione assolutamente antieconomica. E infine (ma non da ultimo), un registro basato su applicativi open source, di cui è possibile verificare le regole che questi implementano e il loro rispetto, nonché di gestire il loro cambiamento nel tempo secondo regole condivise, senza dover chiedere un permesso specifico al titolare del copyright.

Un registro è un registro, una raccolta di dati. Ma è tutto qui? No, perché c'è chi ha fatto un passo oltre e ha rivoluzionato il mondo della Blockchain dando la possibilità di "programmare" alcuni tipi di transazione tramite l'inserimento di codice Turing complete (completo secondo la definizione di Alan Turing, il padre dell'informatica). Vitalik Buterin è chi ha compiuto questo passo: interpretando un pensiero di Nick Szabo, ha infatti implementato gli Smart contract sulla sua Blockchain Ethereum.

Accept

Gli Smart contract, dunque, altro non sono che degli applicativi non esterni inseriti nella Blockchain, i quali, tramite un ambiente “if”, possono autoeseguirsi ed eseguire le operazioni permesse dal codice dello stesso con le limitazioni del linguaggio di programmazione.

Uno Smart contract, dopo essere inserito sulla Blockchain, rimane sulla Blockchain stessa, e al verificarsi delle condizioni per cui è programmato si autoeseguirà, permettendo al programma di far accadere degli eventi programmati/definiti nello stesso. Tutto questo avviene in maniera trasparente, perché il codice sorgente dello Smart contract è disponibile per chiunque ne conosca l’indirizzo, e poi perché è immodificabile, ovvero il codice dello Smart contract stesso è inserito nella Blockchain, che avanzando con la propria “catena di blocchi” renderà non alterabile il blocco dove è contenuto. Seppur a prima vista sembrino degli applicativi che non portano alcun beneficio nella vita di tutti i giorni, gli Smart contract sono potenzialmente rivoluzionari in quanto definiscono in maniera matematica cosa accade quando un determinato evento si verifica, dando così esecuzione automatica al contratto, o a una parte del contratto, e prova dell’esecuzione.

Gli Smart contract possono rendere più facile operazioni di tutti i giorni e, nel contempo, aumentare la fiducia degli utenti che decidono di usarli grazie alla loro immodificabilità e trasparenza.

Alcuni esempi di potenziali applicazioni

Accept

Pensiamo ad alcuni esempi in cui è possibile creare uno Smart contract:

- **La spedizione in contrassegno**: il venditore consegna il pacchetto al vettore, che alla consegna del pacco richiede l'importo all'acquirente, che pagando riceve il pacchetto. Il vettore, poi, paga l'importo al venditore
- **Cambio valute/Exchange:** l'agente di cambio acquista la valuta direttamente dal fornitore, la tiene nel proprio ufficio o luogo preposto al deposito, e l'utilizzatore finale la acquista con la propria valuta pagando un prezzo per tale servizio
- **Acquisto di titoli in borsa:** l'utente deve aprire un portafoglio titoli presso un operatore di borsa, immobilizzare una somma presso l'operatore di borsa, e comunicare all'operatore (anche in via telematica) la condizione per cui acquistare o vendere il titolo di borsa. All'avverarsi della condizione, l'operatore di borsa effettua l'operazione, inserendo il titolo nel portafoglio dell'utente (oppure vendendo il titolo e trasferendo nel portafoglio dell'utente l'ammontare delle somme).
- **Cambiale o assegno circolare:** il debitore compila un titolo secondo cui a una determinata data il creditore potrà riscuoterne il valore. Il creditore a tale data deve recarsi in banca e incassare l'importo, sempre che il debitore non sia insolvente.

Come gli Smart contract possono risolvere e facilitare questi procedimenti

Per il **contrassegno** basterebbe creare uno Smart contract che incameri le somme del bene venduto, e che verificando continuamente lo stato del pacchetto (magari su un'altra Blockchain di dati immodificabile che contenga i dati delle spedizioni), trasferisca automaticamente la somma al venditore quando risulti "consegnato", escludendo quindi la custodia della somma da parte del vettore.

Per l'**exchange** basterebbe uno Smart contract che al ricevimento di una determinata somma converta automaticamente la valuta in un'altra valuta, oppure la scambi con un'altra valuta di un altro portafoglio a cui ha accesso.

Per l'**acquisto di titoli di borsa** è sufficiente uno Smart contract molto semplice a cui sia permesso di analizzare un andamento di un titolo, e che al raggiungimento della cifra impostata acquisti o venda il titolo e lo trasferisca al portafoglio a cui ha accesso.

La **cambiale** o **assegno circolare** su Smart contract è concettualmente ancora più semplice: basterebbe che lo Smart contract sia impostato per congelare un importo trasferito (nel caso dell'assegno circolare), e rilasciarlo a una determinata data futura impostata nel codice, evitando anche il rischio di scoperto per il creditore; oppure che sia impostato per trasferire il determinato importo alla scadenza della cambiale.

Accept

E la validità dei contratti?

Gli Smart contract sono normati in Italia attraverso il Decreto Semplificazioni, che ne ha dato una definizione chiara, attribuendo loro "il requisito della forma scritta previa identificazione informatica delle parti interessate, attraverso un processo avente i requisiti fissati dall'Agenzia per l'Italia digitale". Anche senza tale espresso riconoscimento, dunque in attesa delle norme tecniche, è da ritenersi che, ai sensi dell'attuale normativa sul documento informatico, la registrazione nella Blockchain conferirebbe una garanzia di immodificabilità alle registrazioni tale da costituire uno dei requisiti perché il giudice vi riconosca forma scritta, lasciando al contesto o ad altre forme di prova la necessaria verifica della non ripudiabilità e identificazione delle parti.

Anche in mancanza del riconoscimento della forma scritta, tuttavia, nel diritto contrattuale uno Smart contract sarebbe comunque riconosciuto come un contratto verbale assistito da prova delle "dichiarazioni" contrattuali e dunque del contenuto delle obbligazioni assunte, tra l'altro soffrendo in questo caso molto meno delle incertezze circa l'interpretazione del linguaggio naturale, utilizzando esso un linguaggio più analitico, anzi, autoeseguente.

È chiaro come gli Smart contract creino un ecosistema assolutamente innovativo, e che i governi stiano preparando il terreno fertile per fare sì che gli operatori sviluppino ancora di più sistemi basati su di essi.

Smart contract per tutti gli usi?

Le critiche all'uso della Blockchain e delle soluzioni che si basano su tale tecnologie sono diverse, ma possiamo condensarle in alcuni punti. La Blockchain ha un costo di mantenimento e la registrazione di una transazione ha anch'essa un costo. Pertanto può essere antieconomico utilizzare uno Smart contract per "microtransazioni" con scarso margine. Inoltre, la Blockchain ha una latenza: dall'inserimento della transazione nel pool dei candidati a essere inseriti nel prossimo blocco all'effettivo inserimento passa del tempo. Maggiore la fee riconosciuta a chi inserisce la transazione nel blocco, maggiore la chance che il tempo di latenza sia basso. Pertanto non è possibile avere entrambe le caratteristiche, ovvero una fee bassa e al contempo una transazione in tempi rapidi. Questa caratteristica rende gli Smart contract inadatti per transazioni che siano con scarso margine e che richiedano tempi di latenza bassi o comunque che lo Smart contract si esegua entro un determinato lasso di tempo.

Una critica molto importante che viene sollevata è anche quella dell'enorme e crescente costo che il mantenimento della Blockchain ha sul consumo energetico e dunque sul suo impatto ambientale.

Accept

Tuttavia tale svantaggio è molto accentuato per il Bitcoin, dato il suo valore, meno per altre Blockchain, come Ethereum. Entrambi questi esempi sono basati sulla proof of work (devo dimostrare di aver conferito un rilevante apporto di CPU, dunque di energia), ma altri sono basati su elementi meno energivori, come la proof of stake.

Infine, la carenza di privacy. Le transazioni sono tutte pubbliche, nel senso che tutti possono esaminare quali transazioni un identificativo ha inserito e con chi le ha poste in essere, rendendo non impossibile in determinati casi determinare l'identità reale dell'identificativo, anche se lo stesso di per sé non condurrebbe alla persona fisica o giuridica che ne è titolare (semi-anonimo). Ciò può diffondere in modo irreversibile dati personali, impedendo tra l'altro l'esercizio dell'oblio. L'inserimento della crittografia può almeno in parte risolvere tale problema.

Proprio per tali criticità, c'è chi sostiene che sarebbero preferibili le Blockchain private, ovvero quelle in cui solo alcuni, selezionati operatori sono legittimati a inserire nuovi blocchi e la Blockchain sarebbe alimentabile solo da costoro, mentre i clienti avrebbero solo un'interfaccia da e per la Blockchain, della quale però non possederebbero la copia. Tale soluzione, tuttavia, vanifica una delle caratteristiche di questa tecnologia: essere distribuita (e dunque ispezionabile da chiunque ne abbia interesse), replicabile, nonché alimentabile da chiunque. Non va nemmeno trascurato il fatto che il numero limitato di operatori abilitati a creare la Blockchain, almeno da un punto di vista teorico, incentiva la collusione tra gli operatori al fine di alterare il gioco di creazione competitiva tra più operatori che si contendono le fee per le transazioni. Una via intermedia potrebbe essere quella delle Blockchain ad ammissione, tipo hyperledger fabric di Linux Foundation, ovvero una Blockchain dove può partecipare alla creazione della blockchain solo chi soddisfa determinati requisiti oggettivi ha diritto di essere un nodo che partecipa alla sua creazione.

Infine, come detto, lo Smart contract è una macchina "Turing complete", ma la logica sottesa da una tale macchina non può essere facilmente implementata in contratti al di là di una certa complessità, ma solo in quelli che possono essere descritti tramite un certo numero di transazioni o eventi atomici. Il che ovviamente è vero solo per un insieme molto limitato (ma non per questo irrilevante) di casi.

Conclusioni

La Blockchain è una tecnologia con applicazioni ancora non del tutto comprese nel loro potenziale, ma che ha alcuni punti di forza non indifferenti, sui quali in molti settori vi sono investimenti di notevole importo. Per il loro essere a cavallo tra la tecnologia informatica e la programmazione da un lato e il diritto dall'altro, mettono in comunicazione mondi che solitamente stanno in universi separati. Richiedono, dunque, competenze e capacità di comprendere le implicazioni profonde e le logiche relative in entrambi i campi, e sono in pochi a possederle.

Accept

Tuttavia, in molti ambiti riteniamo saranno indispensabili applicazioni che in certi casi probabilmente ancora non sono state nemmeno concepite.

Giorgio Alessandro Donà Danioni e Carlo Piana

Qualche elemento tecnico di approfondimento: come si realizza un contrassegno sulla blockchain?

Un contrassegno si basa sulla convenzione con il vettore che il venditore riceverà l'importo al momento della consegna all'indirizzo fornito dall'acquirente. L'acquirente quindi invierà la somma allo smart contract, che ne congelerà gli importi fino a quando il pacchetto è ricevuto dall'acquirente. Una volta ricevuto il pacchetto

Vediamo il codice, considerate che la struttura dell'ordine, la struttura dell'indirizzo e i campi relativi all'acquirente sono già impostati. Il codice di esempio è basato su una serie di eventi che devono verificarsi. Ecco gli eventi estratti e riassunti per semplicità. Il codice che segue è stato estratto dal repository Github di Fabio Jose. Il contratto che esaminiamo si articola su tre eventi.

Il primo evento: l'ordine è stato inviato:

```
event OrderSent(address buyer, string goods, uint quantity, uint orderno);
```

Il secondo evento si verifica al pagamento:

```
event SafepaySent(address buyer, uint orderno, uint value, uint now);
```

L'ordine è inviato, il pagamento è inviato, e il pacchetto è in consegna. Lo smart contract è ancora in uno stato intermedio, per chiudere la transazione, manca solo lo sblocco del pagamento. Ciò avverrà al momento della consegna, infatti:

```
event OrderDelivered(address buyer, uint invoiceno, uint orderno, uint
real_delivey_date, address courier);
```

I sopracitati eventi a quel punto faranno sì che si processi il pagamento al venditore, nonché il pagamento della spedizione al corriere, sia nel momento in cui la consegna.

Accept

TAG

BLOCKCHAIN, SMART CONTRACTS

Condividi

Articoli correlati

TECH VISION | 10 SET 2020

Intelligenza Artificiale e Blockchain, un matrimonio inevitabile

L'Intelligenza Artificiale ha una storia che viene da lontano, i primi lavori di rilievo si devono a John McCarthy, Allen Newell e Herbert Simon e sono degli anni '50. I[...]

di MASSIMO CANDUCCI

TECH EXPERIENCE | 11 FEB 2020

Biometria, IoT e Blockchain per identità digitali sicure

"Con la diffusione delle città intelligenti e un numero crescente di sistemi digitalizzati che richiedono l'autenticazione degli utenti, diventa fondamentale pensare a sistemi che possan da un lato agevolare l'operazione[...]

di SONIA MONTEGIOVE

TECH VISION | 7 FEB 2020

Uomo-Macchina, un rapporto che cambia

Accept

Il prossimo decennio sarà caratterizzato da un completo cambio di paradigma nell'interazione tra uomo e macchina e questo avverrà su due direttrici parallele e complementari: l'utilizzo della voce e l'adozione[...]

di MASSIMO CANDUCCI

TECH EXPERIENCE | 28 GEN 2020

Rinnovabili e Banca dell'Energia per salvare il pianeta

In uno studio condotto da 26 ricercatori delle Università di Stanford, Berkeley, Berlino e Aarhus, diretti da Mark Jacobson della Stanford School of Earth, dal titolo "100% Clean and Renewable[...]

di REDAZIONE

AUTORI


Antonio Sagliocca


Claudia Vicari


Eugenio Maddalena


Piersaverio Spinnato


Maurizio Urbani


Mariange Parenti

Accept